PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G07F 7/10

A1

(11) International Publication Number: WO 00/67214

(43) International Publication Date: 9 November 2000 (09.11.00)

(21) International Application Number: PCT/KR00/00406

(22) International Filing Date: 28 April 2000 (28.04.00)

(30) Priority Data:
1999/15282 28 April 1999 (28.04.99) KR
2000/7381 3 April 2000 (03.04.00) KR

(71) Applicant *(for all designated States except US)*: GIFT PD CORPORATION [KR/KR]; 1015 Hyundae Office Building, 9–4 Sunae–dong, Bundang–gu, Kyunggi–do, Sungnam–city 463–020 (KR).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: AHN, Jaesin [KR/KR]; 81–207 Hyundae Apt., 456 Apgujong–dong, Kangnam–gu, Seoul 135–110 (KR).

(74) Agent: KWON, Yong–nam; Yegun Building, 4th floor, 823–42 Yeoksam–dong, Kangnam–gu, Seoul 135–080 (KR).

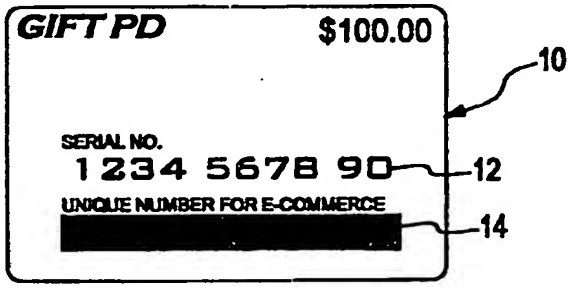
(81) Designated States: JP, US.

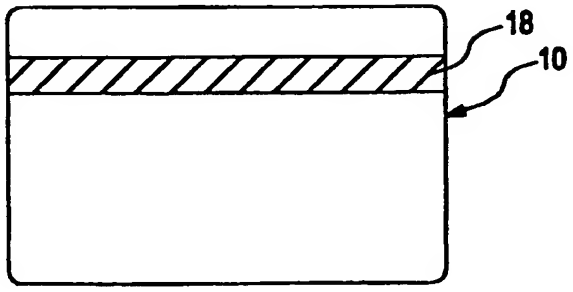
Published
With international search report.

(54) Title: METHOD OF ISSUING PRE–PAID CARD AND METHOD OF AUTHORIZING PRE–PAID CARD AND SUPERVISING BALANCE THEREOF

(57) Abstract

A pre–paid card capable of being received and handled as payment means by a merchant who is not equipped with any dedicated approval terminal, and a method of authorizing the pre–paid cardsupervising the balance of the pre–paid card. According to the preferred embodiment, the pre–paid card (10) has a serial number (12) on its front surface, and two unique numbers one of which is imprinted below the scratch–off material (14) and the other one of which is stored in the magnetic strip (18). The first unique number is used for the authorization of payment in the off–line transaction and the second unique number is used for the authorization of payment in the electronic transaction.





FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

METHOD OF ISSUING PRE-PAID CARD AND METHOD OF AUTHORIZING PRE-PAID CARD AND SUPERVISING BALANCE THEREOF

Technical Field

The present invention relates to a payment system for a commercial transaction. More particularly, the present invention relates to a pre-paid card which is offered before a purchase and system and method for authorizing a transaction using the pre-paid card.

Background Art

A pre-paid card, typically being used as a gift certificate, refers to a card which is offered to a customer with being associated with cash-equivalent value, so that the buyer or recipient thereof may freely spend the amount of value. Generally, the pre-paid card is formed of plastic or polyethylene terephthalate (PET) and has a rectangular shape with a width of about 85 millimeters (mm) and a height of about 54 mm, and its corners being rounded. On the back of the card is included a magnetic strip parallel with an edge thereof for storing a unique number and balance or remaining value so as to facilitate to the use as a gift certificate or payment means. Such a conventional pre-paid card is issued usually by a department store, communications carrier, or the other distributing company having multiple franchise shops.

The conventional pre-paid card, however, may be used at a store which is equipped with a dedicated terminal separately from an authorization terminal for a credit card or a debit card. Accordingly, the merchant who wishes to receive the pre-paid card as payment means experiences an economic burden of buying the terminal. In the viewpoint of the purchaser, it is difficult to conveniently use the card which he or she bought in advance or received from another since the payment by use of the card is available only in the issuer's or its affiliated shop.

Meanwhile, since information stored in the magnetic strip may be read out and recorded easily enough to facilitate a forgery or counterfeiting, the conventional pre-

paid card has a drawback of lacking security severely. In order to overcome the problem, some pre-paid card issuers, e.g., credit card issuing companies or operators of credit card authorizing VAN, provide a unique number or password to the buyer of the card at the time of buying the card instead of recording the unique number in the magnetic strip. However, such cards cause the users thereof inconvenience of inputting the unique number or password through a keypad when purchasing goods or services. So as to reduce the possibility of the forgery or counterfeiting, it may be contemplated to make the pre-paid card to have a form of an IC card or recording a hologram into the card similarly to a credit card. Such an approach is not suitable for the pre-paid card because it increases issuing costs and the pre-paid card is used at most twice or three times.

On the other hand, electronic transaction through the Internet is rapidly growing recently. Several kinds of payment methods, e.g., using credit cards or electronic cash, are used for the electronic transaction. However, the use of the pre-paid card for an electronic transaction as well as an off-line transaction has not been carried out nor proposed yet, which is due to the fact that most of the conventional pre-paid card store the remaining value in the magnetic strip and it is difficult to read out the value without the terminal.

In this regard, network-based electronic cash which is used upon the authorization of a payment broker system carries out, in the on-line transaction, a function of the pre-paid card in the off-line transaction. The user may buy such kind of electronic cash by providing cash or cash equivalent value using the credit card, recharge the remaining value of the account by providing additional cash equivalent value when the remaining value is exhausted, and sell or present the electronic cash to another. However, just as the conventional pre-paid card for the off-line transaction cannot be used for the electronic transaction, the electronic cash can be used only for the electronic transaction but not for the off-line transaction.

Disclosure of the Invention

To solve the above problems, one object of the present invention is to provide a pre-paid card which may be received and handled as payment means by a merchant who is not equipped with any dedicated approval terminal.

Another object of the present invention is to provide a pre-paid card which may be used for an electronic transaction as well as an off-line transaction in the physical world.

Still another object of the present invention is to provide a method of authorizing the pre-paid card supervising the balance of the card for relieving the merchant from the burden of being equipped with a dedicated terminal and reducing any unexpected loss of the owner or the issuer of the card.

Yet still another object of the present invention is to provide a method of authorizing and supervising the balance of the pre-paid card which may be used for an electronic transaction as well as an off-line transaction.

In order to achieve one of the above objects, there is provided a method of issuing a pre-paid card for use in payments in a commercial transaction under authorization and balance supervision of a payment broker system. According to the method, a random number for use in the authorization in the commercial transaction is generated and the information of the random number is recorded in the card body. The card body preferably includes storing means for storing the information of the random number.

In order to achieve another one of the above objects, there is provided a method of issuing a pre-paid card for use in payments in an off-line transaction and an electronic transaction under authorization and balance supervision of a payment broker system. According to the method, a first random number for use in the authorization in the off-line transaction and a second random number for use in the authorization in the electronic transaction are generated and stored in the card body. The card body preferably includes storing means for storing the information of the random number.

In order to achieve still another one of the above objects, there is provided a method of authorizing a pre-paid card for allowing the pre-paid card to be used as payment means for transactions and supervising a balance of the prepaid card, wherein

the pre-paid card has a unique number determined based on a random number which is generated by a random number generator.

First, a terminal for requesting an authorization of the transaction associated with the pre-paid card and a host for storing an issued unique number required to be identical to the first random number are provided. When a user tries to purchase goods by the transaction, the host receives the unique number and a sales amount from the terminal, and compares the unique number and the sales amount with the issued unique number and the balance, respectively.

When the unique number is identical to the issued unique number and the balance is not zero, the transaction using the pre-paid card by an amount is authorized. The amount is the sales amount when the balance is larger than the sales amount, but is the balance when the balance is shorter than the sales amount. In case that the transaction using the pre-paid card is completed, the amount is subtracted from the balance and a subtracted result is stored as an updated balance.

In order to achieve yet still another one of the above objects, there is provided a method of authorizing a pre-paid card for allowing the pre-paid card to be used as payment means for transactions and supervising a balance of the prepaid card. The pre-paid card has a plurality of unique numbers including a first and a second unique numbers determined based on a first and a second random numbers which are generated by a random number generator.

First, there is provided a terminal for requesting an authorization of an off-line transaction associated with the pre-paid card and a host for storing a first and a second issued unique numbers required to be identical to the first and the second random numbers, respectively, and the balance.

When a user tries to purchase goods by the off-line transaction, the host receives the first unique number and a first sales amount from the terminal, and compares the first unique number and the first sales amount with the first issued unique number and the balance, respectively. When the first unique number is identical to the first issued unique number and the balance is not zero, the host authorizes the off-line transaction using the pre-paid card by a first amount. The first amount is the first sales

amount when the balance is larger than the first sales amount, but is the balance when the balance is shorter than the first sales amount.

When the user tries to purchase goods by an electronic transaction, the host receives the second unique number and a second sales amount from a merchant server in which the electronic transaction takes place, and compares the second unique number and the second sales amount with the second issued unique number and the balance, respectively. When the second unique number is identical to the second issued unique number and the balance is not zero, the host authorizes the electronic transaction using the pre-paid card by a second amount. The second amount is the second sales amount when the balance is larger than the second sales amount, but is the balance when the balance is shorter than the second sales amount.

In case that the transaction using the pre-paid card is completed in accordance with the authorization, the first amount or the second amount is subtracted from the balance and a subtracted result is stored as an updated balance.

Brief Description of the Drawings

The above objectives and advantages of the present invention will become more apparent by describing in detail preferred embodiments thereof with reference to the attached drawings in which:

FIG. 1 depicts the front of a pre-paid card, in a state being offered to a customer, according to an embodiment of the present invention;

FIG. 2 depicts the front of the pre-paid card of FIG. 1 when a user removed scratch-off material on the card;

FIG. 3 depicts the back of the pre-paid card of FIG. 1;

FIG. 4 is a flowchart showing the procedure of issuing the pre-paid card shown in FIGS 1 through 3;

FIG. 5 illustrates an example of the data format recorded in the magnetic strip of the pre-paid card according to the present invention;

FIG. 6 illustrates an embodiment of the system for implementing the method of authorizing the pre-paid card and supervising the balance of the pre-paid card, according to the present invention;

FIG. 7 illustrates an example of a card authorization terminal;

FIG. 8 illustrates the procedure of authorizing the pre-paid card in an off-line transaction;

FIG. 9 illustrates an example of the procedure of authorizing the pre-paid card in an on-line transaction; and

FIGS. 10A and 10B illustrate another example of the procedure of authorizing the pre-paid card in the on-line transaction.

Embodiments

FIGS. 1 through 3 shows a pre-paid card according to an embodiment of the present invention. The pre-paid card 10 is formed of plastic or PET and has a rectangular shape with a width of about 85 mm and a height of about 54 mm, and its corners being rounded. A design including the logo or trademark of the issuer and the amount of initial balance is imprinted on the front of the card, and at least of one magnetic strip 18 is disposed on the back of the card in parallel with an upper edge thereof. The issuer of the pre-paid card may be a department store, oil refining company, gas station, book gift certificate seller, or the other kind of distributing company.

In the present embodiment, the pre-paid card 10 is associated with three numbers: one serial number and two unique numbers. As shown in FIGS. 1 and 2, the serial number 12 is lettered on the front of the card 10 and exposed on the outside. The first unique number, which is generated by a random number generator of the card issuer, is stored in the magnetic strip 18. Particularly, in case that the magnetic strip 18 of the pre-paid card is formed in a manner similar to that of a credit card, the first unique number is preferably stored in a track 2, which typically stores credit card information, of three tracks in the strip. The first unique number is used to authorize the card when the owner of the card is to purchase goods or service in an off-line transaction.

The second unique number 16 is generated by the random number generator of the card issuer, also, but is imprinted on the front of the card. Before the card 10 is sold to a buyer, a user-removable scratch-off material 14 is deposited on the imprinted

area. Thus, unless the user removes the scratch-off material, another person cannot know the second unique number 16. The second unique number is used to authorize the card when the owner of the card is to purchase goods or service in an on-line transaction.

FIG. 4 shows a procedure of issuing the pre-paid card shown in FIGS 1 through 3. First, after a card body is provided in step 20, a first and a second random numbers are generated by a random number generator (step 22). As mentioned above, the first random number is to be used for the authorization of the card in the off-line transaction and the second random number is to be used for the authorization of the card in the on-line transaction. Subsequently, the first random number is stored in the magnetic strip 18 and the second random number is imprinted on the card body (steps 24 and 26). Finally, the scratch-off material is deposited over the region on which the second random number is imprinted so as to prevent the second random number from being exposed externally (step 28).

In the present embodiment, since the first and the second random numbers are directly recorded in the magnetic strip 18 and on the front of the card body, the first and the second random numbers correspond to the first and the second unique number 12 and 16, respectively. In an alternative of the present embodiment, however, the first random number may be encrypted before being stored in the magnetic strip 18. In such a case, the encrypted random number will correspond to the first unique number 12.

In another alternative embodiment, the magnetic strip is not provided to the card body 10 and the first unique number 12 is imprinted on the front or back of the card body 10. In such an embodiment, it is preferable to use a PIN pad in the off-line transaction to prevent the first unique number 12 from being exposed to another person. Further, the card body 10 may be fabricated as an IC card or smart card which includes an integrated circuit chip and an antenna. In this case, the first unique number is stored in the integrated circuit chip.

FIG. 5 illustrates an example of the data format recorded in the magnetic strip of the pre-paid card. The recorded data includes an identification alphanumeric (ID) of the card issuer, the unique number of the card, and check bits. In the preferred embodiment, the issuer ID is comprised of eight bytes and denotes the unique code of

the issuer. The unique number of the card is comprised of ten bytes and determined according to the random number generated by the random number generator when the card is issued. The check bits are comprised of two bytes and used for verifying the recorded data. On the other hand, additional data may be included in the data format of FIG. 5 according to the choice of the card issuer or an authorization agency.

Since the unique number of the card is determined based on the random number in the present invention, any two cards having consecutive serial numbers do not reveal any continuity of the unique numbers. Thus, even if somebody reads out the unique number of a card for the purpose of the forgery, he cannot expect the unique number of another card having the serial number near to that of the card which he has read out. For example, assuming that each byte of the unique number denotes a decimal digit, the hitting ratio will be 1/10,000,000,000 when somebody arbitrarily choose a unique number.

FIG. 6 illustrates an embodiment of the system for implementing the method of authorizing the pre-paid card and supervising the balance of the pre-paid card according to the present invention. The system includes a pre-paid card authorization terminal 30, a host of card VAN system 40, a pre-paid card host sub-system 50, and an Internet server of the card issuer 70.

Conventional credit authorization terminal (CAT) already installed at shops honored by any one of credit card companies may be used for the pre-paid card authorization terminal 30. Particularly, since the magnetic strip of the pre-paid card has the same shape as that of the credit card and the unique number is recorded in the second channel similarly to the credit card, simple change of the operating program of the CAT will be enough for adapting the CAT in the handling the pre-paid card without providing additional reading-out head.

FIG. 7 illustrates an example of the CAT 30. The CAT 30 substantially has a shape of a box, and includes a card-swipe slot 32 for receiving the card so that the magnetic strip can be read. The CAT includes, on its top surface, a keypad 34 allowing the merchant to input a type of authorization service request or sold amount. Also, lots of sales slip forms are stacked at the rear of the terminal, so that a sales slip is printed out upon the authorization of the transaction.

When the merchant wishes to request the authorization of the transaction or payment by use of a pre-paid card, the merchant presses a key, "PRE-PAID CARD", inputs sales amount, and presses another key, "TRANSMISSION". Upon the pressure of the transmission key, an authorization request message including the first unique number and the sales amount data is transmitted to the card VAN host 40 through the public switched telephone network (PSTN).

Referring back to FIG. 6, the card VAN host 40, which is an equipment of a card authorization value-added network (VAN) operator, relays authorization requests and response thereto between retailer's terminal and credit card companies. Particularly, the system according to the preferred embodiment of the present invention is implemented based on the infrastructure of conventional credit card authorization system, the card VAN host 40 is connected to a plurality of credit card company's hosts 100A and 100B. Also, the card VAN host 40 is connected to the pre-paid card host sub-system 50 through a dedicated line or a switched network. Thus, the card VAN host 40 can relay authorization requests for pre-paid cards and response thereto between the retailer's CAT 30 and the pre-paid card host sub-system 50.

The pre-paid card host sub-system 50 includes a main computer 52, a database 54, and automatic answering sub-system (ARS) 56. The database 54 stores data of serial numbers, the first and the second unique numbers, initial balances, current balances, and transaction histories for all pre-paid cards issued by card issuers affiliated with the operator of the system 50. Also, the database 54 may additionally store passwords which card holders register through the Internet. Meanwhile, the ARS sub-system 56 is connected to the main computer 52 and allows the card holders to inquire their current balance or remaining value. Also, the ARS sub-system 56 receives and processes card holders' requests of limiting the use of their cards when they lost the cards.

Upon receiving a card authorization request through the card VAN host 40, the main computer 52 compares the first unique number and the sales amount included in the authorization request message with the unique number and the balance stored in the database 54, determines whether to approve the transaction, and transmits response message to the retailer's CAT 30 through the card VAN host 40. In case of approving

the transaction, the main computer 52 subtracts the sales amount from the balance and stores the subtracted amount in the database 54 as the updated balance. At this time, the transaction detail may be stored along with the updated balance.

A pre-paid card issuer's Internet server 70 is provided for each of the card issuers. Personnel of the card issuing companies can transmit data of serial numbers, the first and the second unique numbers, and initial balances of all the cards issued by the companies to the pre-paid card host sub-system 50 through his or her terminal connected to the server 70. Also, the personnel can check the balance of each card issued by the company from the pre-paid card host sub-system 50. Alternatively, the pre-paid card host sub-system 50 may report the balance of each card issued by each company to the card issuer's Internet server 70 periodically or non-periodically. For the interaction between the pre-paid card host sub-system 50 and the card issuer's Internet server 70, the pre-paid card host sub-system 50 may provide a user name and password, for accessing the pre-paid card host sub-system 50, to each card issuer.

The card holder may access the Internet server 70 using the web browser installed in his or her client computer 84. The card issuer's Internet server 70 may provide a CGI window for inputting a password for payments in electronic transaction in response to an HTML request from the client computer 84. After the card holder inputs desired password along with the serial number of his card and the like, the card issuer's Internet server 70 transmits the password to the pre-paid card host sub-system 50 so that the main computer 52 stores the password in the database 54.

Some of the issuers of the pre-paid cards according to the present invention may operate her own cyber shopping mall. The Internet server of such a company carries out the card issuing and administrating tasks along with the function of a merchant server. Considering the load and computing power of the server, however, the card issuing company may be equipped with a plurality of computers separately for card issuing and administrating function and function of the merchant server.

When purchasing goods in the Internet server 70 of the card issuer, the card holder may pay for his ordering by use of the pre-paid card. For facilitating this payment, the Internet server 70 provides a button of "PAYMENT BY PRE-PAID CARD" as one of optional payment methods in an HTML or ASP page for the

payment. If the card holder chooses the payment by the pre-paid card, the card issuer's Internet server 70 makes the card holder input the password and the second unique number, and transmits the password, the second unique number, and the sales amount to the pre-paid card host sub-system 50 to seek the approval of the transaction. The other feature of the authorizing procedure in the electronic transaction is similar to that in the off-line transaction.

On the other hand, the pre-paid card according to the present invention may be utilized when the holder purchases goods or services from shopping malls 72A and 72B other than the card issuer's Internet server 70. The shopping malls 72A and 72B allowing the payment by use of the pre-paid card may be arranged by contracts between the operator of the pre-paid card host sub-system 50 or the card issuer's Internet server 70 and the operators of the shopping malls. Since the procedures of ordering, payment and card authorization in the shopping malls 72A and 72B are similar to those in the shopping mall operated by the card issuer's Internet server 70, the detailed description thereof will be omitted.

As described above, the shopping mall 70, 72A, or 72B receives the password and the second unique number and transmits such data to the pre-paid card host sub-system 50 to be authorized in the preferred embodiment. In an alternative of the embodiment, however, when the card holder clicks the buttons of "PAYMENT BY PRE-PAID CARD" and "CONFIRMATION", the web browser is connected to the pre-paid card host sub-system 50 of which address is hyper linked to the "CONFIRMATION" button. At this time, the Uniform Resource Location (URL) of the hyper linked web page of the pre-paid card host sub-system 50 includes the sales amount as a header.

The card holder may input the password and the second unique number to an input window in the web page provided by the pre-paid card host sub-system 50. The main computer 52 compares the password, the second unique number, and the sales amount with those stored in the database 54. Upon completion of the comparison, an authorization result ASP page is transmitted to the client computer 84. The authorization result ASP includes a message notifying the authorization result and a button of "RETURN TO SHOPPING MALL". If the card holder clicks the button of

"RETURN TO SHOPPING MALL", the web browser is redirected to the shopping mall server 70, 72a, or 72b and the payment procedure is completed. When the transaction session is completed, the shopping mall server 70, 72a, or 72b transmits a payment completion message to the main computer 52, so that the balance data in the database 54 is updated. Meanwhile, Cookies may be utilized so as to facilitate the return to the shopping mall.

The configuration and operation of the shopping mall for the electronic transaction, the page move utilizing the hyperlink text, the utilization of Cookies are well known to those skilled in the art, specifically in the Internet-related business field. Therefore, the detailed descriptions thereof will be omitted.

Now, the procedure of authorizing transaction payments using the pre-paid card in the off-line transaction and the electronic transaction will now be described, in more detail, with reference to FIGS. 8 through 10B.

FIG. 8 illustrates the procedure of authorizing the pre-paid card in the off-line transaction. When the purchaser wishes to pay by the pre-paid card, the merchant swipes the card in the CAT 30 to read out data stored therein, inputs sales amount, and presses "TRANSMISSION" button (step 100). Accordingly, the authorization request message including the ID of the card issuer, the first unique number, and the sales amount is transmitted to the VAN host 40 (step 102). Recognizing that the message is concerned with the pre-paid card, the VAN host 40 forwards the received data to the main computer 52 of the pre-paid card host sub-system 50 (step 104). The main computer 52 decodes the received data and checks the first unique number and balance stored in the database 54 (step 106).

The main computer 52 compares the first unique number included in the authorization request message with that from the database 54 to determine whether they are the same to each other. Upon completion of the determination, the main computer 52 transmits an authorization response message to the CAT 30 via the VAN host 40 (steps 108 and 110).

In case that the first unique number in the authorization request message is identical to that stored in the database 54 and the balance is larger than the sales amount, the authorization response message includes the balance data along with the

approval information. In case that the first unique number in the authorization request message is identical to that stored in the database 54 but the balance is shorter than the sales amount, the authorization response message includes information notifying the deficit of the balance and the amount of the balance. If the balance is deficient as such, the purchaser may pay the amount of the balance by the pre-paid card and the remaining amount by cash or the credit card. On the other hand, in case that the first unique number in the authorization request message is different from that stored in the database 54, the authorization response message includes the request to call back and report to the police along with information that the card is illegal.

In response to the authorization response message approving the transaction, the CAT 30 generates receipt and displays the balance of the card (step 112). Afterwards, the CAT 30 reports the transaction result to the main computer 52 of the pre-paid card host sub-system 50 via the VAN host 40 (steps 114 and 116). The pre-paid card host sub-system 50 updates the database 54 by changing the balance reflecting the transaction result and by adding the transaction result (step 118).

On the other hand, the main computer 52 of the pre-paid card host sub-system 50 periodically reports lists of card-receipts of each merchant and the balance of each card to the card issuer's Internet server 70. Also, a portion of such data may be provided to the VAN host operator and/or the retailer merchants (step 120). The card issuer pays, to each of the retailer merchants, the payment amount handled by the merchant periodically or non-periodically. The payment of the card issuer may be carried out by the operator the pre-paid card host sub-system 50, the VAN host operator, or the other affiliate of the issuer in place of the issuer.

FIG. 9 illustrates an example of the procedure of authorizing the pre-paid card in the on-line or electronic transaction. When wishing to purchase goods or services by the electronic transaction, the purchaser first accesses the shopping mall 70, 72a, or 72b which accepts the payment by the pre-paid card of the present invention. For the reference of consumers, each shopping mall 70, 72a, or 72b may indicate, in its homepage, whether the mall accepts the pre-paid card. After ordering goods or services into the shopping cart, the purchaser may click the "PAYMENT" button to proceed to the payment stage (step 130).

The web page for the payment includes a plurality of buttons for selecting one of optional payment method, which include the button of "PAYMENT BY PRE-PAID CARD". If the purchaser clicks the "PAYMENT BY PRE-PAID CARD" button in step 132, the shopping mall requests the purchaser to input the password and the second unique number (step 134). If the purchaser inputs the password and the second unique number and clicks the "CONFIRMATION" button, the password and the second unique number are transmitted to the shopping mall 70, 72a, or 72b (step 136).

Receiving the password and the second unique number, the shopping mall 70, 72a, or 72b transmits the authorization request message including the passsword, the second unique number, and the sales amount to the pre-paid card host sub-system 50 (step 138). The main computer 52 compares the password and the second unique number included in the authorization request message with those from the database 54 to determine the validity (step 140). Also, the main computer 52 determines whether the sales amount is smaller than the balance. Upon completion of the determination, the main computer 52 transmits an authorization response message and balance data to the shopping mall 70, 72a, or 72b (step 142).

In response to the authorization response message approving the transaction, the shopping mall 70, 72a, or 72b transmits a message to the client computer 84 informing the completion of the payment (step 144). Subsequently, the shopping mall 70, 72a, or 72b reports the transaction result to the main computer 52 of the pre-paid card host sub-system 50 (step 146). The main computer 52 of the pre-paid card host sub-system 50 updates the database 54 by changing the balance reflecting the transaction result and by adding the transaction result (step 148).

On the other hand, the main computer 52 of the pre-paid card host sub-system 50 periodically, e.g., once a month, reports lists of card-receipts of each shopping mall and the balance of each card to the card issuer's Internet server 70 (step 150). Based on the report, The card issuer pays, to each of the shopping malls, the payment amount handled by the mall periodically or non-periodically (step 152). Similarly to the off-line transaction, the payment of the card issuer may be carried out by the operator the pre-paid card host sub-system 50, the VAN host operator, or the other affiliate of the issuer in place of the issuer.

FIGS. 10A and 10B illustrate another example of the procedure of authorizing the pre-paid card in the on-line transaction. In the example of FIG. 9, the shopping mall 70, 72a, or 72b directly receives the password and the second unique number from the client computer 84 and transmits such data to the main computer 52 to get the approval. On the contrary, in the example of FIGS. 10A and 10B, if the purchaser wishes to pay by the pre-paid card, the client computer 84 is directed to the main computer 52 so that the main computer 52 receives the password and the second unique number.

First, the purchaser may click the "PAYMENT" button to proceed to the payment stage after selecting desired goods or services in the same way as the example of FIG. 9 (step 160). Here, if the purchaser clicks the buttons of "PAYMENT BY PRE-PAID CARD" in step 162, a message of "... moving to authorization site" is displayed on the web browser and cookies information for returning later to the shopping mall is downloaded to the web browser to be stored in the client computer 84 (step 164). Afterwards, the web browser is connected to the main computer 52. At this time, the URL of the hyper linked web page provided by the shopping mall for the connection to the pre-paid card host sub-system 50 includes the sales amount in its header (step 166).

After the main computer 52 asks the purchaser to input the password and the second unique number in step 168 and the purchaser inputs the password and the second unique number accordingly and clicks the "CONFIRMATION" button, the password and the second unique number are transmitted to the pre-paid card host sub-system 50 (step 170). The main computer 52 compares the password and the second unique number included in the authorization request message with those from the database 54 to determine the validity (step 172). Also, the main computer 52 determines whether the sales amount is smaller than the balance. Upon completion of the determination, the main computer 52 transmits an authorization response message and balance data to the client computer 84 (step 174).

When the purchaser clicks the button of "RETURN TO SHOPPING MALL" in step 176, provided in the received web page, the web browser is redirected to the shopping mall server 70, 72a, or 72b in step 178. Next, the shopping mall server

carries out payment processing and transmits a payment completion message to the client computer 84 (step 180). Since the procedure shown in steps 182 through 188 in FIG. 10B is similar to that shown in the steps 146 through 152 in FIG. 9, the detailed description thereof will be omitted.

On the other hand, in order to prevent the second imprinted under the scratch-off material from being exposed, which may result in illegal use of another person, various kinds of provisions may be contemplated. First, it is necessary to promote or educate the card holder who seldomly use electronic transactions not to scratch off the material. When the card holder lost or was robbed of the card, the lawful owner may report the fact to the pre-paid card host sub-system 50 through the Internet or the ARS sub-system 56, present his or her password or the second unique number, and ask to prevent the use by others in the off-line transaction. In such a case, the lawful owner may continue to use the card in the electronic transaction. Also, the pre-paid card host sub-system 50 may register the name, citizen's registration number or social security number, and E-mail address of the lawful owner along with the owner's password. In such a case, the robber or the finder of the card cannot rashly try to be granted his own password using the second unique number imprinted on the card.

Also, the pre-paid card host sub-system 50 may request to change certain digits (e.g., last four digits) of the second unique number whenever a new electronic transaction is completed or started so as to prevent the second unique number from hacking and enhance the reliability of data transmission. Also, in another alternative, a plurality of second unique numbers may be imprinted on the card and only one of the numbers is used under the direction of the system.

Although the present invention has been described in detail above, it should be understood that the foregoing description is illustrative and not restrictive. Those of ordinary skill in the art will appreciate that many obvious modifications can be made to the invention without departing from its spirit or essential characteristics.

In case of a high denomination card, for example, the buyer of the card may be provided with another password in addition to the serial number and the first and the second unique numbers, so that the card holder has to input the password in a PIN pad connected to the CAT. Such a password may be required in checking the balance

through the ARS sub-system 56 as well. Also, the data transmission may be protected by use of a security algorithm to prevent the hacking of transmitted data.

Even though the CAT for the credit card was exemplified as the card authorization terminal In the above description of the preferred embodiments, other kinds of terminals may be used to read the card in another embodiments of the present invention. Also, a point-of-sale (POS) terminal may be used instead of the CAT in a large distribution center such as a department store.. In such a case, data read out by the POS terminal may be transmitted directly to the pre-paid card host sub-system 50 detouring the card VAN host 40, which enables the terminal operator to save the connection fee to be paid otherwise.

The card holder can recharge or increase the balance of the card by paying cash-equivalent value, e.g., by using the credit card, in a state of being connected to the pre-paid card host sub-system 50 or the card issuer's Internet server 70 through the Internet. Such alternatives may easily be implemented by one those skilled in the art, and thus the description of details of the alternatives will be omitted. Also, the system supporting the recharging may provide points or mileages to users who frequently use the card in the off-line transaction and electronic transaction. Owing to the capability of being recharged, the pre-paid card according to the present invention may be expanded to an extent of electronic cash.

Even though the card VAN host 40 and the main computer 52 of the pre-paid card host sub-system 50 are illustrated as single computers, each of those computers may be comprised of a plurality of computers in the physical configuration. On the other hand, the card VAN host 40 and the pre-paid card host sub-system 50 may be operated by the same business entity, in which case, both systems may be implemented in a single hardware. Similarly, the pre-paid card host sub-system 50 and the card issuer's Internet server 70 may be operated by the same business entity, in which case, both systems may be implemented in a single hardware, also.

In the above description, it was described that the card issuer produces the pre-paid cards. Actually, however, the card issuing company and the card manufacturer may be separate business entities. In such a case, the card manufacturer just performs the simple processing of recording the serial number and random numbers provided by

the card issuing company to the card body. Thus, in the case that the card issuing company is different from the card manufacturer, the term "card issuer" should be construed to be the company which entrusts the manufacturer with producing the cards sells the produced cards, and the action of the manufacturer should be construed to be done by the card issuer.

In the preferred embodiments, the pre-paid card includes two unique numbers: one for the off-line transaction and the other one for the electronic transaction. In the other embodiment, however, the pre-paid card may include just a single unique number, which may be dedicated to the off-line transaction or may be used for the electronic transaction as well as the off-line transaction.

Having described and illustrated the principles of the invention in preferred embodiments and alternatives thereof, it should be apparent that the invention can be modified in arrangement and detail without departing from such principles. We claim all modifications and variation coming within the spirit and scope of the following claims.

Industrial Applicability

According to the present invention, the authorization of the pre-paid card is not required for the off-line transaction and can be performed using conventional credit card authorization terminals. Accordingly, the use of the pre-paid card is not limited to stores equipped with dedicated terminals. Rather, the card may be used in the transaction at any places, for example, a small-sized supermarket, a restaurant, or a gas station, in which the credit card authorization terminal is installed. Thus, the burden of the stores honored by the card issuer of being equipped with the dedicated terminal is relieved. Also, in the viewpoint of the purchaser, the utility of the pre-paid card is increased.

Even when a unique number of a pre-paid card is read out illegally, it is substantially impossible to expect the unique numbers of another card having serial numbers adjacent to that of the read-out card because the first and the second unique numbers are based on random numbers from the random number generators. Further,

when a single card is counterfeited or forged, the loss of the card issuer is not so critical because the initial balance or value of a pre-paid card is not so high.

Also, the present invention assigns and manages two unique numbers for a single card, and thus the purchaser can conveniently exploit the off-line transaction and the electronic transaction using a single card.

What is claimed is:

1. A method of issuing a pre-paid card for use in payments in a commercial transaction under authorization and balance supervision of a payment broker system, wherein the method comprises the steps of:

(a) providing a card body;

(b) generating a random number for use in the authorization in the commercial transaction; and

(c) recording information of the random number in the card body.

2. The method as claimed in claim 1, wherein said step (a) comprises the step of providing storing means in the card body,

wherein said step (c) comprises a step of (c1) storing information of the random number in the storing mens.

3. The method as claimed in claim 2, wherein the information of the random number is identical with the random number, so that the random number itself is stored in the storing means in said step (c).

4. A method of issuing a pre-paid card for use in payments in an off-line transaction and an electronic transaction under authorization and balance supervision of a payment broker system, wherein the method comprises the steps of:

(a) providing a card body;

(b) generating a first random number for use in the authorization in the off-line transaction and a second random number for use in the authorization in the electronic transaction; and

(c) recording information of the first random number and the second random number in the card body.

5. The method as claimed in claim 4, wherein said step (a) comprises the step of providing storing means in the card body,

wherein said step (c) comprises a step of (c1) storing information of the first random number in the storing mens.

6. The method as claimed in claim 5, wherein the information of the first random number is identical with the first random number, so that the first random number itself is stored in the storing means in said step (c).

7. The method as claimed in claim 5, further comprising the step of:
encrypting the first random number before performing said step (c),
wherein the encrypted random number is stored in said step (c).

8. The method as claimed in claim 5, wherein said step (c) further comprises the steps of:

(c2) imprinting the second random number on the front of the card body; and

(c3) depositing scratch-off material over the region on which the second random number is imprinted so as to prevent the second random number from being exposed externally.

9. A method of authorizing a pre-paid card for allowing the pre-paid card to be used as payment means for transactions and supervising a balance of the prepaid card, wherein the pre-paid card has a unique number determined based on a random number which is generated by a random number generator, wherein said method comprises the steps of:

(a) providing a terminal for requesting an authorization of the transaction associated with the pre-paid card and a host for storing a issued unique number required to be identical to the first random number, respectively, and the balance;

(b) when a user tries to purchase goods by the transaction, receiving the unique number and a sales amount from the terminal, and comparing the unique number and the sales amount with the issued unique number and the balance, respectively;

(c) when the unique number is identical to the issued unique number and the balance is not zero, authorizing the transaction using the pre-paid card by an amount,

wherein the amount is the sales amount when the balance is larger than the sales amount

wherein the amount is the balance when the balance is shorter than the sales amount; and

(d) in case that the transaction using the pre-paid card is authorized in said step (c), subtracting the amount from the balance and storing a subtracted result as a updated balance.

10. A method of authorizing a pre-paid card for allowing the pre-paid card to be used as payment means for transactions and supervising a balance of the prepaid card, wherein the pre-paid card has a plurality of unique numbers including a first and a second unique numbers determined based on a first and a second random numbers which are generated by a random number generator, wherein said method comprises the steps of:

(a) providing a terminal for requesting an authorization of a off-line transaction associated with the pre-paid card and a host for storing a first and a second issued unique numbers required to be identical to the first and the second random numbers, respectively, and the balance;

(b) when a user tries to purchase goods by the off-line transaction, receiving the first unique number and a first sales amount from the terminal, and comparing the first unique number and the first sales amount with the first issued unique number and the balance, respectively;

(c) when the first unique number is identical to the first issued unique number and the balance is not zero, authorizing the off-line transaction using the pre-paid card by a first amount,

wherein the first amount is the first sales amount when the balance is larger than the first sales amount,

wherein the first amount is the balance when the balance is shorter than the first sales amount;

(d) when the user tries to purchase goods by an electronic transaction, receiving the second unique number and a second sales amount from a merchant server in which

the electronic transaction takes place, and comparing the second unique number and the second sales amount with the second issued unique number and the balance, respectively;

(e) when the second unique number is identical to the second issued unique number and the balance is not zero, authorizing the electronic transaction using the pre-paid card by a second amount,

wherein the second amount is the second sales amount when the balance is larger than the second sales amount,

wherein the second amount is the balance when the balance is shorter than the second sales amount; and

(f) in case that the transaction using the pre-paid card is authorized in said step (c) or (e), subtracting the first amount or the second amount from the balance and storing a subtracted result as a updated balance.

11. The method as claimed in claim 10, wherein said step (a) comprises the step of providing the pre-paid card with means for storing information.

12. The method as claimed in claim 11, wherein the information storing means includes a magnetic strip deposited thereon.

13. The method as claimed in claim 11, wherein the terminal is selected from a credit authorization terminal for authorizing a credit card and a POS terminal.

14. The method as claimed in claim 11, wherein the first unique number is stored in the information storing means and the second unique number is imprinted on a surface of the pre-paid card.

15. The method as claimed in claim 10, wherein the second unique number is identical with the second random number.

16. The method as claimed in claim 10, further comprising the step of:

(g) notifying the balance to the user in response to a request of the user.

17. The method as claimed in claim 10, wherein the pre-paid card is associated with a predetermined password,

wherein, in said step (d), the host additionally receives the password from the user through the merchant server,

wherein, in said step (e), the host authorizes the electronic transaction using the pre-paid card only when the password is correct.

FIG. 1

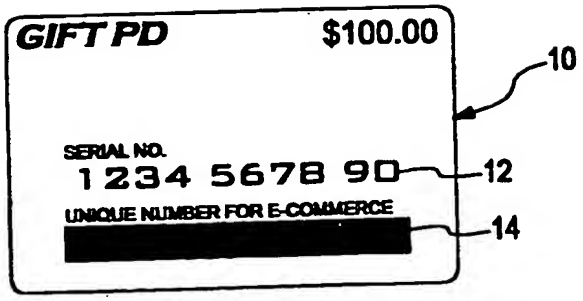


FIG. 2

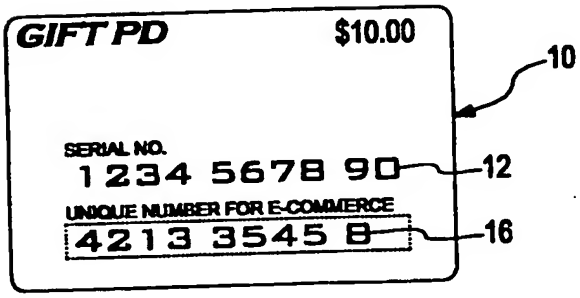


FIG. 3

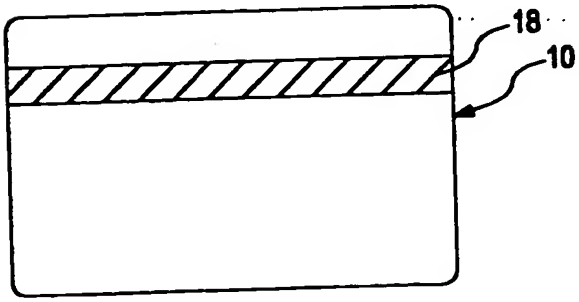


FIG. 4

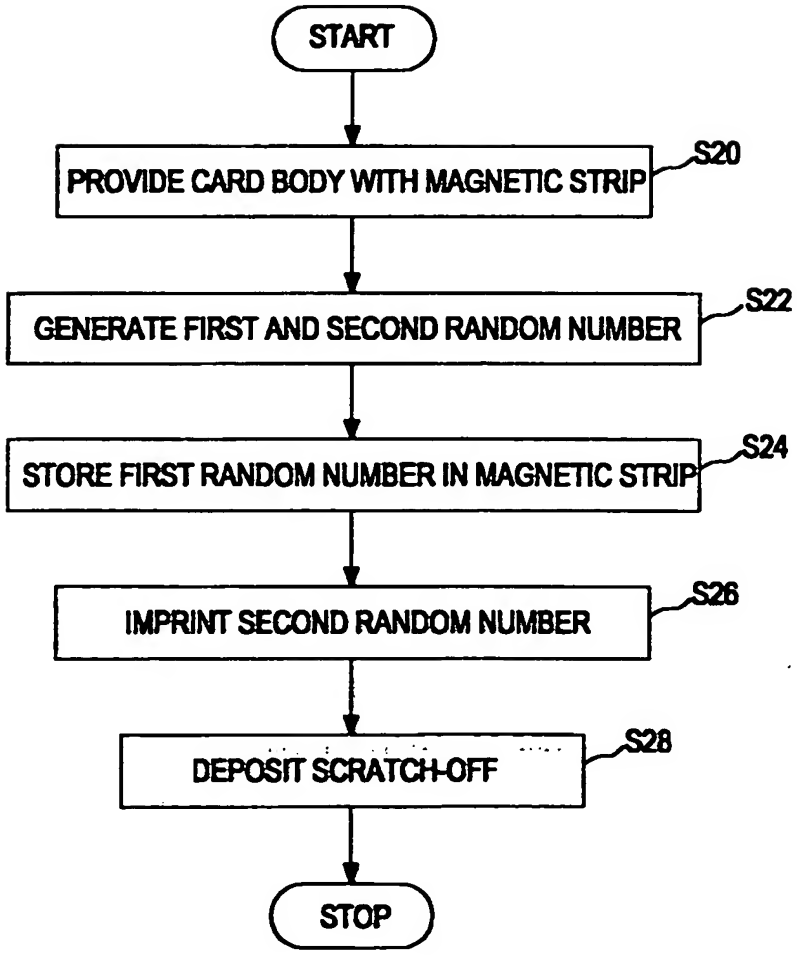
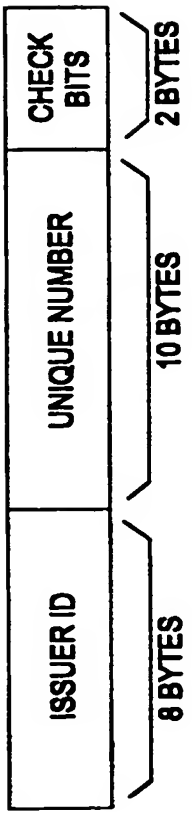

START
PROVIDE CARD BODY WITH MAGNETIC STRIP
S20
GENERATE FIRST AND SECOND RANDOM NUMBER
S22
STORE FIRST RANDOM NUMBER IN MAGNETIC STRIP
S24
IMPRINT SECOND RANDOM NUMBER
S26
DEPOSIT SCRATCH-OFF
S28
STOP

FIG. 5



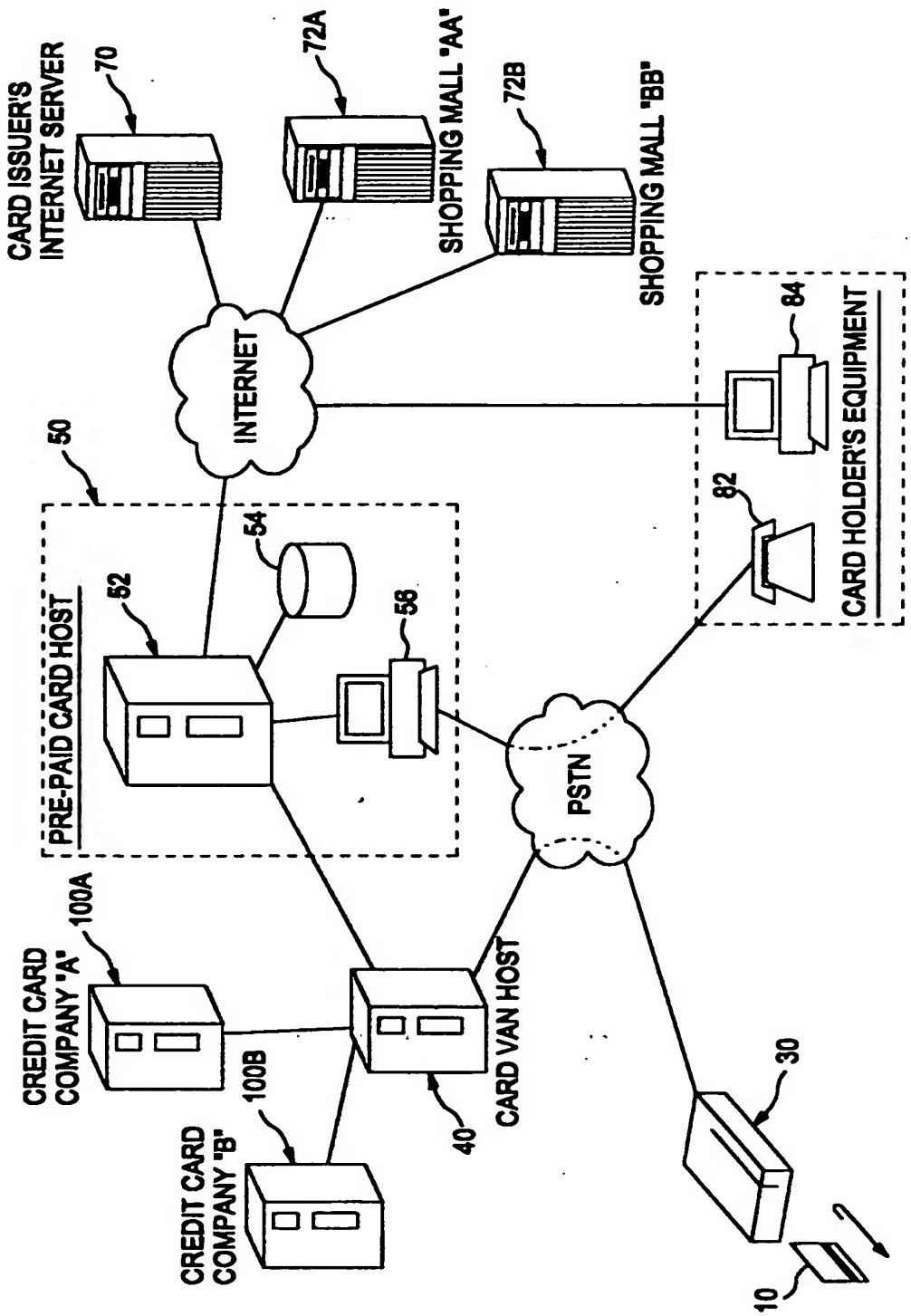

CARD ISSUER'S INTERNET SERVER
70
72A
SHOPPING MALL "AA"
72B
SHOPPING MALL "BB"
INTERNET
84
CARD HOLDER'S EQUIPMENT
82
50
54
52
PRE-PAID CARD HOST
58
PSTN
100A
CREDIT CARD COMPANY "A"
100B
CREDIT CARD COMPANY "B"
40
CARD VAN HOST
30
10

FIG. 6

FIG. 7

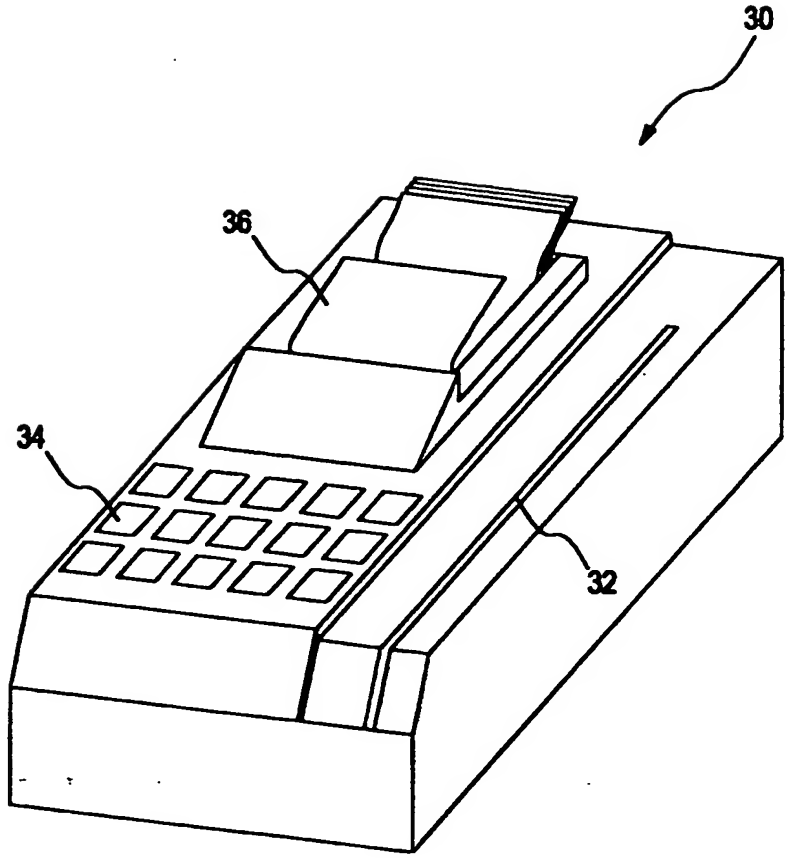


FIG. 8

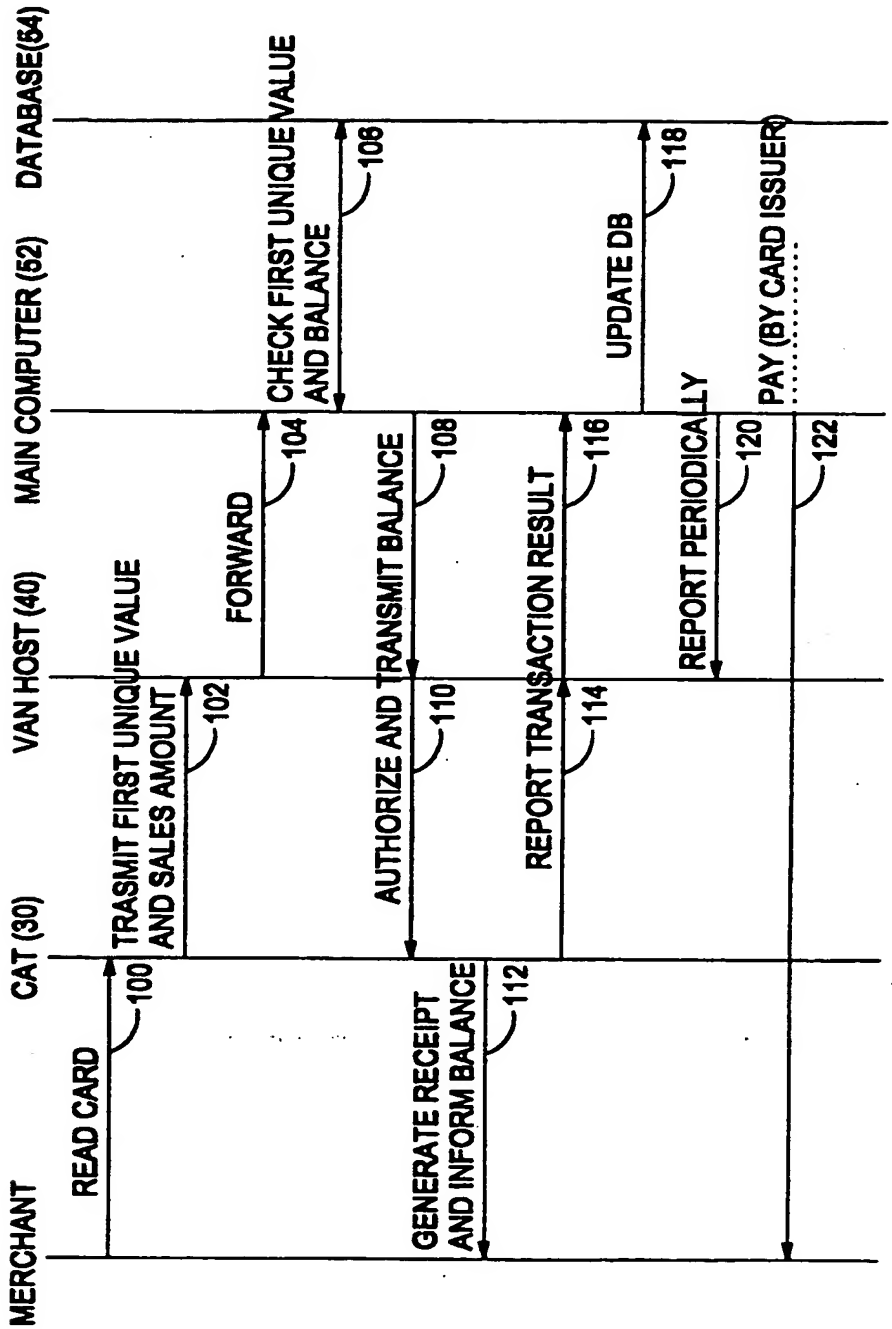

MERCHANT
CAT (30)
VAN HOST (40)
MAIN COMPUTER (52)
DATABASE(64)
READ CARD
100
TRASMIT FIRST UNIQUE VALUE AND SALES AMOUNT
102
FORWARD
104
CHECK FIRST UNIQUE VALUE AND BALANCE
106
AUTHORIZE AND TRANSMIT BALANCE
108
110
REPORT TRANSACTION RESULT
114
116
UPDATE DB
118
REPORT PERIODICALLY
120
PAY (BY CARD ISSUER)
122
GENERATE RECEIPT AND INFORM BALANCE
112

FIG. 9

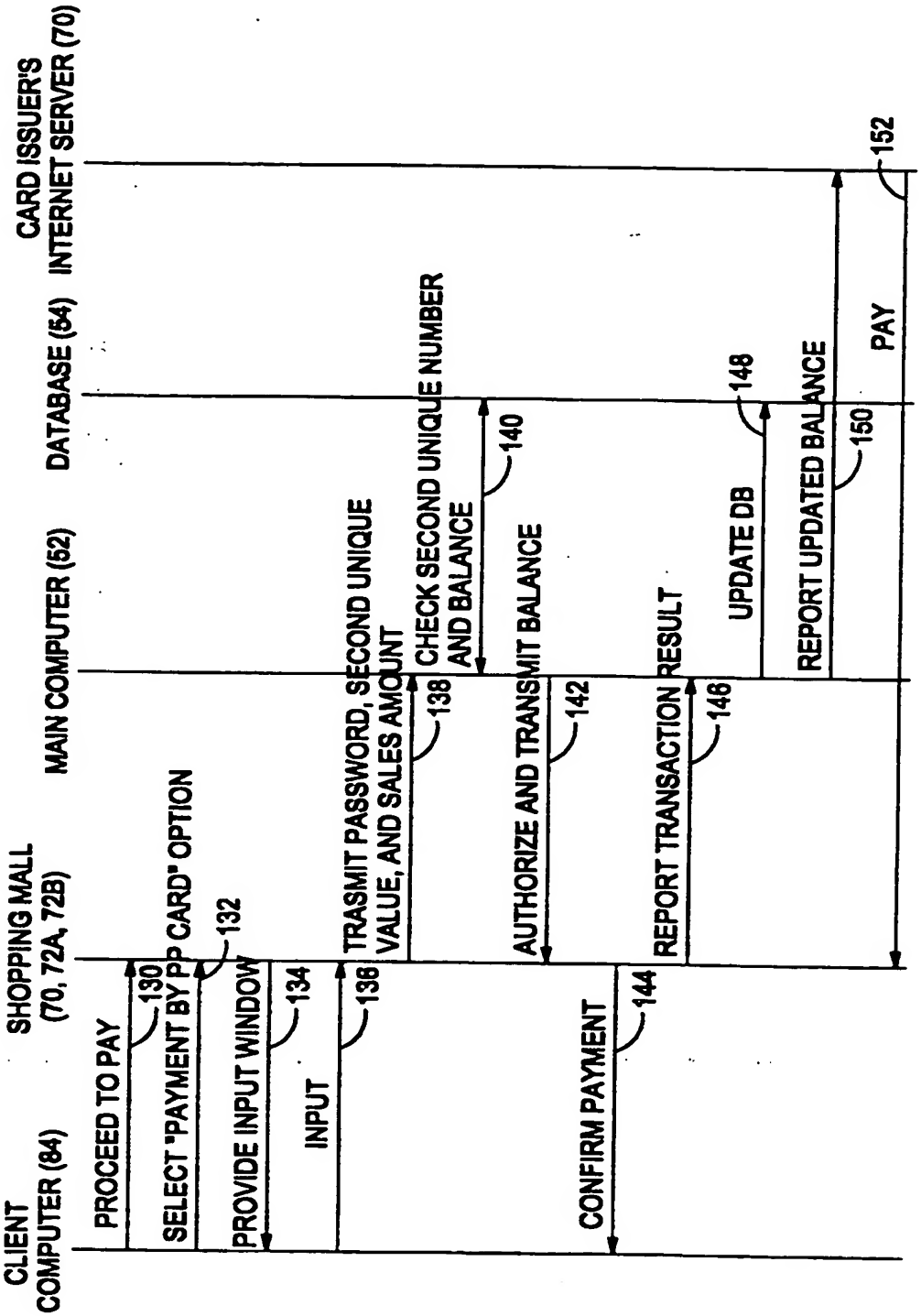

CLIENT COMPUTER (84)
SHOPPING MALL (70, 72A, 72B)
MAIN COMPUTER (62)
DATABASE (64)
CARD ISSUER'S INTERNET SERVER (70)
PROCEED TO PAY
130
SELECT "PAYMENT BY PP CARD" OPTION
132
PROVIDE INPUT WINDOW
134
INPUT
136
TRASMIT PASSWORD, SECOND UNIQUE VALUE, AND SALES AMOUNT
138
CHECK SECOND UNIQUE NUMBER AND BALANCE
140
AUTHORIZE AND TRANSMIT BALANCE
142
CONFIRM PAYMENT
144
REPORT TRANSACTION RESULT
146
UPDATE DB
148
REPORT UPDATED BALANCE
150
PAY
152

FIG. 10A

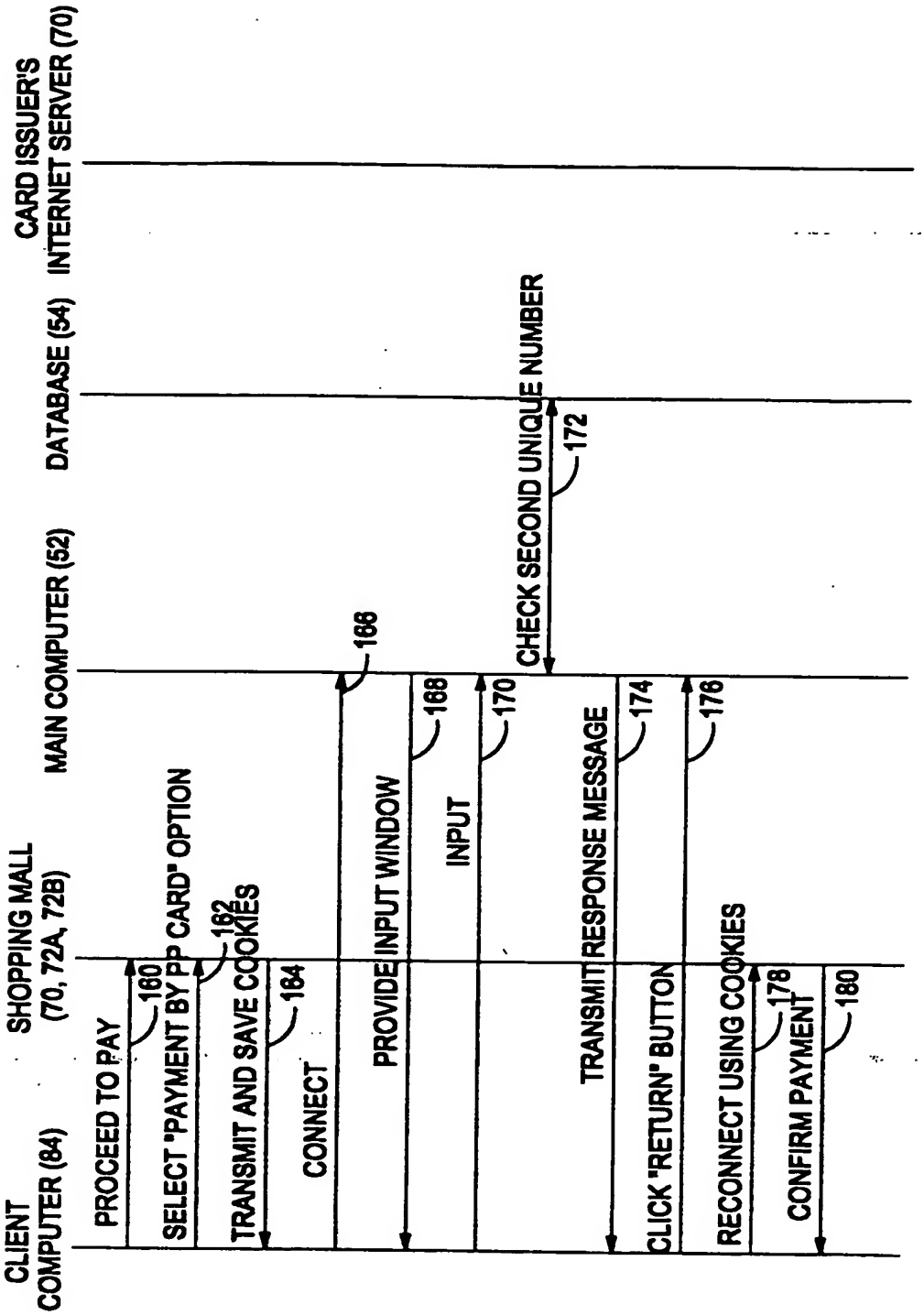
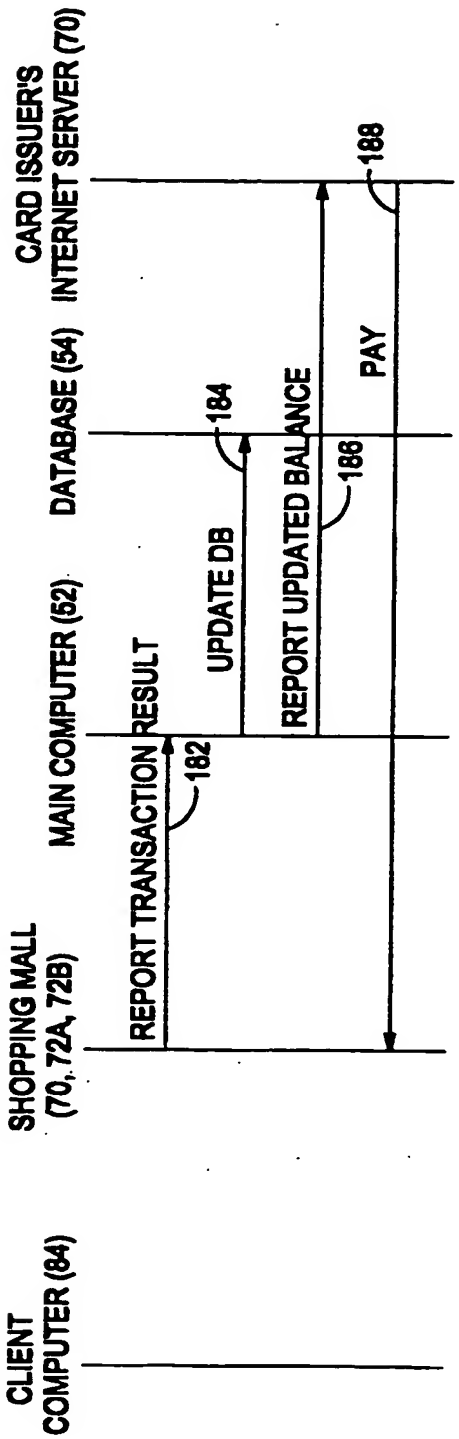

CLIENT COMPUTER (84)
SHOPPING MALL (70, 72A, 72B)
MAIN COMPUTER (52)
DATABASE (54)
CARD ISSUER'S INTERNET SERVER (70)
PROCEED TO PAY
160
SELECT "PAYMENT BY PP CARD" OPTION
182
TRANSMIT AND SAVE COOKIES
184
CONNECT
186
PROVIDE INPUT WINDOW
188
INPUT
170
CHECK SECOND UNIQUE NUMBER
172
TRANSMIT RESPONSE MESSAGE
174
CLICK "RETURN" BUTTON
176
RECONNECT USING COOKIES
178
CONFIRM PAYMENT
180

FIG. 10B


CLIENT COMPUTER (84)
SHOPPING MALL (70, 72A, 72B)
MAIN COMPUTER (62)
DATABASE (54)
CARD ISSUER'S INTERNET SERVER (70)
REPORT TRANSACTION RESULT
182
UPDATE DB
184
REPORT UPDATED BALANCE
186
PAY
188

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR 00/00406

A. CLASSIFICATION OF SUBJECT MATTER

IPC[7]: G 07 F 7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC[7]: G 06 F 15/30, G 06 K 5/00, G 06 K 19/00, G 07 F 7/00, G 07 F 7/10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

USPTO

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5786587 A (COLGATE, JR.) 28 July 1998 (28.07.98) abstract; column 3, line 63 - column 5, line 18; column 6, line 60 - column 8, line 26; fig. 1-5.	1 - 17
A	US 4839504 A (NAKANO) 13 June 1989 (13.06.89) abstract; column 3, line 43 - column 4, line 68; column 8, line 45 - column 9, line 20; claims 1-8; fig. 2,8A,8B.	1 - 17
A	US 4745267 A (DAVIS et al.) 17 May 1988 (17.05.88) abstract; claims 1-12; fig. 1-7.	1 -17
A	US 5293029 A (IIJIMA) 08 March 1994 (08.03.94) abstract; claims 1,2; fig. 1.	1 - 17

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
„A" document defining the general state of the art which is not considered to be of particular relevance
„E" earlier application or patent but published on or after the international filing date
„L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
„O" document referring to an oral disclosure, use, exhibition or other means
„P" document published prior to the international filing date but later than the priority date claimed
„T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
„X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
„Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
„&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 June 2000 (23.06.00)	16 August 2000 (16.08.00)
Name and mailing adress of the ISA/AT Austrian Patent Office Kohlmarkt 8-10; A-1014 Vienna Facsimile No. 1/53424/535	Authorized officer Stanger Telephone No. 1/53424/182

Form PCT/ISA/210 (second sheet) (July 1998)

The Document US-A-5,786,587 discloses a chip card, such as a financial transaction card, having first identifying data written in a read-only memory portion of circuitry contained in the card, wherein second and third identifying data are respectively coded in a machine readable optically variable device (e.g., a hologram) and a magnetic stripe on the card. The authenticity of the card is verified by combining these different identifying data; for example, the second and third identifying data may be combined to produce an algorithm which is compared with the first identifying data for authentication of the card.

The document US-4,839,504 discloses an IC card system, wehrein a first file corresponding to a normal bank account and a second file corresponding to an IC card account are provided for each IC cardholder. A card terminal for receiving an IC card communicates in an on-line manner with a host computer installed in a bank. A deposit amount is transferred between the first and second files for a transaction using the IC card. The IC card stores an account list for the transfer of a remittance to an account of a third party, so that a cash transfer from the first or second file to the account of the third party can be performed. The IC card functions both as a debit card and a credit card. When either of these functions is selected, an off-line transaction involving use of the IC card can be performed.

The document US-4,745,267 discloses credit card blanks which are manufactured with a plurality of random, secure codes (24) such as randomly applied infrared readable bits. A card encoding apparatus (B) includes a secure code reader (32) for reading the secure code from one of the blanks. The secure code and account information are operated on by an encoding algorithm (36, 38) to generate a verification code which is electromagnetically recorded (40) or embossed (42) on the card. In conjunction with a credit card transaction, the merchant passes the credit card past an electromagnetic read head (50) and an infrared read head (52) to read the electronically encoded account information, verification code, and secure code. A keyboard (54) enables the merchant to manually enter this data if the electromagnetic recording should be unreadable. The verification apparatus operates on the account information with a verification algorithm (66, 68, 70) to generate an answer corresponding to the verification code. If the answer and verification code match, an authentication code generator (82) generates an authentication code which is displayed on an LCD dot matrix display (56) and handwritten by the merchant on the receipt.

The document US-5,293,029 discloses a mutual certification method that includes an IC card having a random number generator, a plurality of key data and a plurality of encryption algorithms, and an IC card terminal which also has a random number generator, a plurality of key data and a plurality of encryption algorithms. The key data and encryption algorithm to be used are designated, and a random number may be transmitted for encryption and return, so that mutual certification may be performed.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/KR 00/00406

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US A 5786587	28-07-1998	AU A1 67207/96	05-03-1997
		BR A 9610044	21-12-1999
		CA AA 2229215	20-02-1997
		EP A1 870278	14-10-1998
		WO A1 9706507	20-02-1997
US A 4839504	13-06-1989	JP A2 63032658	12-02-1988
US A 4745267	17-05-1988	AU A1 38341/85	12-07-1985
		EP A2 152703	28-08-1985
		EP A3 152703	19-08-1987
		JP T2 61500876	01-05-1986
		US A 4626669	02-12-1986
		WO A1 8502927	04-07-1985
US A 5293029	08-03-1994	FR A1 2641885	20-07-1990
		FR B1 2641885	27-01-1995
		GB A0 8929239	28-02-1990
		GB A1 2227111	18-07-1990
		GB B2 2227111	19-05-1993
		HK A1 1003129	09-10-1998
		JP A2 2187888	24-07-1990
		JP A2 2187785	23-07-1990